

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

----- x

UNITED STATES OF AMERICA,

- against -

10 Cr. 1082 (TPG)

ABDULE QAYAM DURRANI,

Defendant.

----- x

SENTENCING MEMORANDUM OF THE UNITED STATES OF AMERICA

PREET BHARARA
United States Attorney for the
Southern District of New York
One Saint Andrew's Plaza
New York, New York 10007
Telephone: (212) 637-1945/2482
Facsimile: (212) 637-2452
E-mail: matthew.schwartz@usdoj.gov
negar.tekeei@usdoj.gov

MATTHEW L. SCHWARTZ
NEGAR TEKEEI
Assistant United States Attorneys
- Of Counsel -

The United States of America (the “Government”), by and through its attorney Preet Bharara, United States Attorney for the Southern District of New York, respectfully submits this memorandum in advance of the sentencing of Abdul Qayum Durrani (“Durrani” or the “defendant”) in the above-captioned case, presently scheduled for January 7, 2013 at 4:30 p.m.

PRELIMINARY STATEMENT

Abdul Qayum Durrani was part of an international conspiracy that was responsible for stealing the bank account information of hundreds of thousands of consumers and using the stolen information to create counterfeit ATM cards to withdraw cash from those people's accounts. They stole account information primarily in Europe, and they used the stolen account information to extract cash from ATMs throughout the world, including in the Southern District of New York, as well as in Europe, the Middle East, the Far East, the Caribbean, and elsewhere. In or about April 2011, Durrani traveled from the United Kingdom to the Netherlands, along with his co-defendants Mohammed Khawar (“Khawar”), Fassel Azim (“Azim”), and David Smith (“Smith”), in order to install these manipulated card readers at stores throughout Holland. Once in the Netherlands, Durrani, Khawar, Azim and Smith entered several stores to install manipulated card readers. In view of the role that Durrani played in a massive fraud, a Guidelines sentence is both appropriate and necessary in this case.

BACKGROUND

A. The Scheme to Defraud¹

From at least 2007 until at least the summer of 2011, the Khan Family Organization was an international criminal organization principally in the business of stealing credit card, bank

¹ The facts in this section are drawn from Durrani's Presentence Investigation Report (“PSR”), as well as from the second superseding Indictment in this case, *United States v. Irfan Khan, et al.*, No. S2 10 Cr. 1082 (TPG).

account, and related financial information from consumers at retail establishments; using the stolen account information to extract cash from automated teller machines (“ATMs”) using counterfeit ATM cards; and laundering the proceeds of the scheme back to its organizers. (PSR ¶ 23; Ind. ¶¶ 2, 84). The Khan Family Organization (or simply, the Organization) — which has at various times been based out of the United Kingdom, the United Arab Emirates, and the Netherlands — developed an especially technologically sophisticated method of fraudulently obtaining customer account data from retail locations. (Ind. ¶ 3). As described below, members and associates of the Khan Family Organization were dispatched throughout the United Kingdom, mainland Europe, and elsewhere to install credit card reader devices that had been customized to steal users’ account information, through the addition of particularly advanced “skimmers.” (PSR ¶¶ 23-24; Ind. ¶ 3).

The Organization’s leadership then dispatched members and associates of the Organization throughout the world — including to New York City, the United Kingdom, mainland Europe, Southeast Asia, the Middle East, Africa, the Caribbean, South America, Australia, and elsewhere — to create counterfeit ATM cards using the stolen account information and to fraudulently withdraw cash from victims’ accounts. (Ind. ¶ 4). Members and associates of the Organization then laundered the proceeds of the fraud back to its leadership through various means, including by physically carrying cash internationally; through structured Western Union or similar transactions; and through the informal system of banking known as hawala or its functional equivalent. (Ind. ¶ 5).

To the Government’s knowledge, the Khan Family Organization was one of the largest, if not the single largest, credit card skimming syndicates throughout the world. The hallmarks of

the Khan Family Organization were its technological sophistication, its enormous scale, and its organizational discipline.

Technological Sophistication. “Skimmers” frequently consist of a small device that fits over the slot through which the customer swipes an ATM or credit card, accompanied by a hidden camera that records the customer entering his or her personal identification numbers (“PIN”). (Ind. ¶¶ 16-17). Using such crude technology, a skimming device can typically be installed for only a short period of time — typically a few hours — before being removed by the individual engaged in the account theft. The thief must then manually review the video footage to match customers’ PINs (obtained by video) with the corresponding account information (obtained through the skimmer). (*Id.*).

The Khan Family Organization, however, developed a skimmer that fit entirely *inside* of the card reader terminal (known as a PIN entry device, or “PED”), and which was able to intercept both the customer’s card number and PIN automatically. (Ind. ¶ 27). (The Organization’s skimmer, moreover, worked for both American-style magnetic stripe cards and European-style chip and PIN “smartcards.”) The skimmer was then connected to what was essentially the guts of a cellphone, so that the stolen account and PIN data could be sent via text message to members of the Organization. (PSR ¶ 24; Ind. ¶ 31). In this way, the Organization’s skimmers were able to run uninterrupted for weeks or months at a time, stealing every customer’s information and sending it to members of the Organization in a form ready to be used. (*Id.*). As a result, a single skimmer could (and did) easily steal information pertaining to thousands or even tens of thousands of bank accounts. (PSR ¶ 27; Ind. ¶¶ 18, 24-25).

Scale of Operations. Of course, the Organization did not operate a single skimmer. Rather, having perfected its technology, the Organization began to mass produce its skimmers for installation into PEDs in retail locations throughout Europe. (PSR ¶ 24; Ind. ¶ 33). Although the full scope of the Organization may never be known, the evidence gathered during the course of the Government's investigation reveals its enormity:

- In 2008, a member of the Organization's leadership contacted various electronics and software purveyors in Britain to source component parts to manufacture the Organization's skimmers, ordering, for example, 900 modems and 1,300 circuit boards. (PSR ¶ 24; Ind. ¶¶ 34-36).
- Between April 2008 and March 2009, a secure FTP site used by the Organization to receive the text messages containing stolen accounts and PINs received approximately 350,000 transfers of data, representing approximately the number of accounts compromised by the Khan Family Organization over that period. (PSR ¶ 28; Ind. ¶ 48).
- In early 2009, a pair of police seizures from Khan Family Organization premises in London resulted in the seizure of almost a thousand PEDs in various stages of alteration. (PSR ¶ 26; Ind. ¶¶ 37-41).
- In early 2010, Irfan Khan and Zeshan Mian were arrested in Holland carrying a memory device that contained, among other things, approximately 186,000 unique stolen bank account numbers and their associated PINS. (PSR ¶ 27; Ind. ¶ 67).

In short, the Khan Family Organization operated on a massive scale. (See PSR ¶¶ 23-24).

Organizational Discipline. Notwithstanding the size and geographical scope of the Organization's operations, the Organization's core membership itself was never especially large. The Organization's leadership, moreover, insisted upon strict operational discipline wherein only a very few co-conspirators were trusted with information that would actually allow them, for example, to fraudulently obtain cash. For instance, although the Organization employed "cashers" throughout the world to use the stolen account information to obtain cash from ATMs,

(Ind. ¶¶ 4, 49), those cashers often were not provided with that stolen account information. Rather, the Organization's leadership transmitted the stolen data to more trusted organizers, who created counterfeit ATM cards and assigned them to cashers. (Ind. ¶¶ 50-52). But neither the cashers nor even the local organizer were given the corresponding PINs that were necessary to use the stolen cards. Rather, cashers were required to speak to other members of the Organization located in "call centers," principally located in Pakistan and the United Arab Emirates, who would give out the PINs one by one, as the cashier was required to report the results of each card. (Ind. ¶ 53). In that way, the Organization's leadership kept careful account of how much cash was obtained from each counterfeit card, and no single person had all of the tools — data, ATM card, and PIN — necessary to commit the crime.

B. The Defendant's Offense Conduct

In April 2011, Abdul Qayam Durrani, the defendant, traveled from the United Kingdom to the Netherlands, along with co-defendants Khawar, Azim, and Smith, in order to install these manipulated card readers at stores throughout Holland. (PSR ¶ 33; Ind. ¶ 81). They brought with them, among other things, a laptop computer that contained account information stolen a year earlier by other co-conspirators in Holland, and skimmers built to Irfan Khan's specifications. *Id.* Once in the Netherlands, Durrani, Khawar, Azim, and Smith also obtained three PED terminals, to use as non-functioning dummies. *Id.* In the Netherlands, Durrani, Khawar, Azim and Smith entered several stores to install manipulated card readers, including a shoe store in Utrecht. *Id.*

C. The Indictment, Durrani's Extradition to the United States, and His Guilty Plea

On or about September 1, 2011, a grand jury in this District returned the S1 Indictment, charging Durrani in four counts, including charges of conspiracy to commit bank and wire fraud,

conspiracy to commit access device fraud, conspiracy to commit international money laundering, and aggravated identity theft. (S1 10 Cr. 1082 (S1 Indictment) ¶¶ 1, 7, 15, 18). On or about July 13, 2012, Durrani was extradited from the United Kingdom to the United States to face these charges. On or about November 15, 2013, a grand jury in this District returned the S2 Indictment, charging Durrani in four counts, including charges of conspiracy to commit bank and wire fraud, conspiracy to commit access device fraud, conspiracy to commit international money laundering, and aggravated identity theft. (PSR ¶¶ 2, 5, 9, 10). On July 25, 2013, Durrani pleaded guilty before the Honorable Gabriel W. Gorenstein, pursuant to a plea agreement. (PSR ¶ 14).

Under the terms of the plea agreement, Durrani was permitted to plead guilty to Count One, which charges conspiracy to commit bank and wire fraud, and Count Four, which charges conspiracy to commit access device fraud. The parties also agreed on the application of the United States Sentencing Guidelines (“Guidelines” or “U.S.S.G.”). Among other things, the parties agreed that:

- The bank and wire fraud objects of Count One are grouped with one another and with the access device fraud objects of Count Four. *See* U.S.S.G. § 3D1.2.
- The base offense level for the group is 7. *See* U.S.S.G. §§ 2X1.1, 2B1.1(a)(1).
- A 20-level enhancement is appropriate because the loss reasonably foreseeable to Durrani was more than \$7,000,000, but not more than \$20,000,000. *See* U.S.S.G. § 2B1.1(b)(1)(K).
- A 2-level enhancement is appropriate because (a) Durrani participated in relocating the fraudulent scheme to another jurisdiction to evade law enforcement or regulatory officials (*i.e.*, from the United Kingdom to the Netherlands), *and* (b) a substantial part of the fraudulent scheme was committed from outside the United States; *and* (c) the offense otherwise

involved sophisticated means. *See* U.S.S.G. § 2B1.1(b)(10).

- A 2-level enhancement is appropriate because the offense involved (a) the possession or use of any (i) device-making equipment (*i.e.*, the credit card writer and associated software), or (ii) authentication feature (*i.e.*, the stolen PINs); *and* (b) the production of any (i) unauthorized access device or counterfeit access device, or (ii) authentication feature. *See* U.S.S.G. § 2B1.1(b)(11).

Assuming Durrani accepted responsibility for his crimes, therefore, the parties agreed that the total offense level on Count Four of the Indictment was 28. Because Durrani has never lived in the United States, he has no American criminal history. (PSR ¶¶ 42-44). Accordingly, Durrani is in Criminal History Category I and the parties therefore stipulated that the appropriate Guidelines sentencing range for Durrani's offense is 78 to 97 months' imprisonment.

DISCUSSION

A. A Guidelines Sentence Is Appropriate

A criminal sentence must be crafted to adequately reflect, among other things, the seriousness of the offense, the need for respect for the law, and the need to punish the offense and deter future criminal conduct. *See* 18 U.S.C. § 3553(a)(2). Based on the Guidelines calculations contained in the parties' plea agreement and in the PSR, the applicable Guidelines range is 78 to 97 months' imprisonment.

Although the Guidelines are of course no longer mandatory, the Supreme Court has made clear that a sentencing court should "consult" the Guidelines and "take them into account" when sentencing. *United States v. Booker*, 543 U.S. 220, 264 (2005). The Court has recently reaffirmed that the Sentencing Commission "continues to fill an important institutional role because it has the capacity courts lack to base its determinations on empirical data and national experience, guided by a professional staff with appropriate expertise. Accordingly, we have

instructed that district courts must still give respectful consideration to the now-advisory Guidelines (and their accompanying policy statements).” *Pepper v. United States*, — U.S. —, 131 S.Ct. 1229, 1247 (2011) (internal quotation marks, citations, and alterations omitted). Indeed, “a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range,” which “should be the starting point and the initial benchmark.” *Gall v. United States*, 552 U.S. 38, 49 (2007); *see also United States v. Cavera*, 550 F.3d 180, 189 (2d Cir. 2008) (en banc) (“Even after *Gall* and *Kimbrough*, sentencing judges, certainly, are not free to ignore the Guidelines, or to treat them merely as a ‘body of casual advice.’” (quoting *United States v. Crosby*, 397 F.3d 103, 113 (2d Cir. 2005))).

Here, a Guidelines sentence is the right one. First and foremost, a Guidelines sentence is necessary to reflect the seriousness of Durrani’s offense. Durrani knowingly joined an international credit card fraud conspiracy, traveling with his co-defendants from the United Kingdom to Holland in order to install manipulated card readers at stores throughout Holland. In the course of one trip in April 2011, Durrani and his co-defendants entered several stores to install the manipulated card readers. The intended losses were more than \$7,000,000. In his sentencing submission, Durrani argues that was a minor player in the conspiracy in that he agreed to be a part of the conspiracy during its last week of operation, and that his “actions in the Netherlands resulted in no stolen access devices.” In April 2011, Durrani and his co-conspirators traveled from the United Kingdom to the Netherlands with a laptop computer containing stolen access devices, materials to alter access device readers, including three GSM modules, and tools to alter access device readers. (Plea Transcript at 14 (allocution).) During that trip, he and his co-conspirators entered stores in the Netherlands intending to steal the stores’ access device readers and replace them with counterfeit readers. (*See id.* at 15.) Durrani’s

co-conspirator during the trip, Fassel Azim, who pleaded guilty pursuant to a plea agreement and faced a Guidelines range of 46 to 57 months' imprisonment for his role in the offense, was sentenced by Your Honor to a term of 46 months' imprisonment. The Government submits that the Guidelines range for Durrani, as reflected in the plea agreement and in the PSR's recommendation, appropriately accounts for Durrani's role.

A Guidelines sentence is also necessary to deter future criminal conduct. The Organization of which Durrani was a part was extraordinarily sophisticated. They disseminated stolen account information to cashers throughout the world, but concentrated on the United States because its financial institutions are generally consumer-friendly. It was precisely because U.S. banks seek to please their customers — by having so many bank branches, by allowing large ATM transactions, and by permitting free movement throughout the country and often the world without presuming fraud on the part of the consumer — that the Organization targeted banks in New York City. A Guidelines sentence is necessary in order to send the message that America will not allow its financial institutions to be victimized in this way. A Guidelines sentence would also communicate that, regardless of who bears the ultimate financial loss, America will not tolerate crimes committed on its soil. That the Organization (although not Durrani) specifically relocated from Europe to the United States to take advantage of what it perceived to be easy victims and disinterested law enforcement only underscores the need for a sentence that will serve the goals of promoting respect for the laws and deterring future criminal conduct.

Durrani's crime was a serious one, both in its own right and because his conduct occurred in the midst of a global financial crisis, when European financial institutions were particularly unstable. As a result, Durrani is a defendant for whom a Guidelines sentence is necessary to

afford adequate deterrence generally to criminal conduct and protect the public from his further crimes, as well as to reflect the seriousness of the offense and provide just punishment. *See* 18 U.S.C. § 3553(a)(1), (2)(A), (B) and (C).

B. Effect of Durrani's Prior Incarceration

Durrani seeks a reduction of his sentence “by fifteen months and two days to account for his incarceration in the Netherlands” for acts related to the conduct charged in the Indictment. (Durrani’s Sentencing Letter at 8.) Under 18 U.S.C. § 3585(b), in calculating a sentence, “[a] defendant shall be given credit toward the service of a term of imprisonment for any time he has spent in official detention prior to the date the sentence commences . . . as a result of the offense for which the sentence was imposed . . . that has not been credited against another sentence.” This calculation, however, is done by the Bureau of Prisons, and need not be incorporated into the defendant’s sentence by, for example, reducing his sentence by the time spent imprisoned abroad. *See, e.g., United States v. El-Jassem*, 819 F. Supp. 166, 182 (E.D.N.Y. 1982) (Weinstein, J.) (“Defendant will receive credit for time served in Italy [awaiting extradition] in accordance with United States federal lenient practice. The computation of time served will be made by the Attorney General.” (citing *United States v. Wilson*, 503 U.S. 329 (1992))). Therefore, the Government respectfully submits that Durrani’s prior incarceration should not factor into the sentence imposed by the Court, as the Bureau of Prisons will evaluate Durrani’s prior incarceration in the Netherlands and determine the amount of time, if any, he should be given as credit toward his sentence here.

CONCLUSION

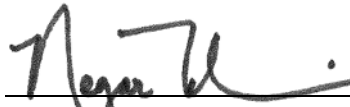
For the foregoing reasons, the Government submits that a Guidelines range sentence is appropriate in this case. In addition, the Court should impose orders of restitution and forfeiture, consistent with the recommendation contained in the PSR, copies of which will be provided to the Court at sentencing.

Dated: January 3, 2014
New York, New York

Respectfully submitted,

PREET BHARARA
United States Attorney

By:

A handwritten signature in dark ink, appearing to read "Negar Tekeei", is written over a horizontal line.

MATTHEW L. SCHWARTZ
NEGAR TEKEEI
Assistant United States Attorneys
One Saint Andrew's Plaza
New York, New York 10007
Telephone: (212) 637-1945/2482
Facsimile: (212) 637-2452
E-mail: matthew.schwartz@usdoj.gov
negar.tekeei@usdoj.gov